



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,415	02/01/2002	Ahmet Mursit Eskicioglu	RCA 89462	3679
7590	01/20/2011		EXAMINER	
Joseph S Tripoli Thomson Multimedia Licensing Inc PO Box 5312 Princeton, NJ 08543-5312			CHAI, LONGBIT	
			ART UNIT	PAPER NUMBER
			2431	
			MAIL DATE	DELIVERY MODE
			01/20/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/936,415	Applicant(s) ESKICIOGLU ET AL.
	Examiner LONGBIT CHAI	Art Unit 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 November 2010.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-24 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 01 February 2002 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1448)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION (RCE)

1. Presently, pending claims are 1 – 8, 10, 14 and 17 – 24.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/22/2010 has been entered.

Response to Argument

3. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.
4. Applicant argues the combination of VCR 130 in Tsuria (Figure 1 / Element 130) with the terminal unit (or replay device) in En-Seung (Figure 4 / Element 21b) because (a) the server in En-Seung does not receive the scramble program from a *service provider* and the terminal unit (or replaying device) in En-Seung does not correspond to the recited *rebundled descrambling key*, as recited in claim 1 (Remarks: Page 11 – 13) and (b) (a) the VCR 130 in Tsuria merely acts as a vehicle for storing the scrambled (or encrypted) digital data stream (SDDS) without providing decryption functions (Remarks: Page 10 – 11). Examiner respectfully disagrees with the following rationale.

- Based upon the Principles of Patent Law, (a) According to MPEP §2145, one cannot show non-obviousness by attacking references *individually* where the rejections are based on combinations of references. See Keller, 642 F.2d at 425 and (b) The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference, but rather, the test is what the combined teachings of those references would have suggested to those of ordinary skill in the art regarding the claim limitations 1 (a) – (e). See Keller, 642 F.2d at 425.

✓ In light of that, the teaching of the primary reference Tsuria that Examiner's reliance on is (a) receiving the scramble program from a *service provider* (Tsuria: Column 3 Line 1 – 8 and Figure 1) and (b) the TECM key (i.e. Transformed ECM key) is qualified as a *rebundled descrambling key* (Tsuria: Column 5 Line 42 – 55: descrambling the content key (i.e. *control word*) from the ECM and re-scrambling / transforming into a TECM key) for later decrypting the scrambled content).

✓ Regarding this subject matter, both of the Tsuria and En-Seung references disclose a recording device for later playback the encrypted digital content and the content key, which decrypts the scrambled digital content, is encrypted by a user key (i.e. TECM key) in Tsuria (Column 8 Line 59 – 62: the *TECM* key is personal to a particular user) and in En-Seung (Abstract / Line 10 – 16 and Column 16 Line 42 – 51: the *temporary validation key* is encrypted by a registered user key).

✓ However, Tsuria teaches that the second device VCR 130 merely stores the re-scrambled digital content which is encrypted with a *rebundled descrambling key* (i.e. *TECM key*) but VCR 130 does not receive the TECM key for descrambling the content and thus it requires the VCR 130 to pass back the encrypted digital content back to the first device IRD for decryption upon user's playback (Tsuria: Column 9 Line 30 –

36) but Tsuria also indicates that any other appropriate digital device can be used in place of the second device VCR 130 (Tsuria: Column 7 Line 13 – 18).

✓ Examiner notes it would have been obvious with *common sense* at the time the invention was made to combine the teaching of En-Seung with Tsuria reference because En-Seung provides an improved and more efficient mechanism to allow the users to view / replay the digital content at their convenience wherein the terminal unit (or the replay device) is capable to directly descrambled the protected digital content by using an decryption key (i.e. temporary validation key), which is encrypted by a user key (or *corresponding to TECM key in Tsuria*), without the need to transfer the received / encrypted digital content back to the first device for decrypting and replaying the recorded digital content (En-Seung: Abstract / Line 10 – 16 and Column 16 Line 42 – 51 & Figure 23B).

✓ Thereby, Examiner has articulated as a rationale the improvement of the primary reference Tsuria *by the teaching* of the secondary reference En-Seung and as such Applicant's arguments are respectfully traversed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1 – 5, 7, 8, 10, 14, 17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (U.S. Patent 6,178,242), in view of En-Seung et al. (U.S. Patent 6,892,306).

As per claim 1, 10 and 21, Tsuria teaches a method for managing access, within a network comprising a first device interconnected to a second device, the method comprising:

(a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key (Tsuria: Column 3 Line 1 – 8 and Figure 1: the first device is interpreted as the IRD (Integrated Receiver Decoder) on Figure 1 / Element 110 and the second device is interpreted as the playback device (or VCR) on Figure 1 / Element 130 capable to record and present data for display on the monitor);

(b) rebundling, in said first device, said descrambling key using a unique key associated with said first device (Tsuria: Column 3 Line 1 – 8 and Column 8 Line Line 59 – 52 / Line 53 – 55: i.e. TECM key (Transformed ECM key), as taught by Tsuria, which could be generated based upon a user key or a combination of apparatus / device IRD (i.e. the access device)).

Tsuria teaches receiving, in said second device, said scrambled data component (Tsuria: Column 9 Line 30 – 36) and generated a rebundled descrambling key (i.e. TECM key) (Tsuria: Column 5 Line 42 – 55) as an encryption key to scramble the digital content.

However, Tsuria does not explicitly disclose receiving, in said second device, said rebundled descrambling key (or encryption key). En-Seung (& Tsuria) teaches:

(c) receiving, in said second device, said scrambled data component and said rebundled descrambling key (or encryption key) (En-Seung: Abstract / Line 10 – 16 and Column 16 Line 42 – 51 & Figure 23B, Column 2 Line 6 – 8, Column 4 Line 58 – 63, Column 3

Line 9 – 13, Column 6 Line 37 – 40 / Line 8 – 13, Column 1 Line 19 – 20: En-Seung provides an improved and more efficient mechanism to allow the users to view / replay the digital content at their convenience wherein the terminal unit (or the replay device) is capable to directly descrambled the protected digital content by using an decryption key (i.e. temporary validation key), which is encrypted by a user key (or *corresponding to TECM key in Tsuria*), without the need to transfer the received / encrypted digital content back to the first device for decrypting and replaying the recorded digital content).

It would have been obvious to a person of ordinary skill *having common sense* in the art at the time the invention was made to combine the teaching of En-Seung within the system of Tsuria because (a) both of the Tsuria and En-Seung references disclose a recording device for later playback the encrypted digital content and the content key, which decrypts the scrambled digital content, is encrypted by a user key (i.e. TECM key) in Tsuria (Column 8 Line 59 – 62: the TECM key is personal to a particular user) and in En-Seung (Abstract / Line 10 – 16 and Column 16 Line 42 – 51: the temporary validation key is encrypted by a registered user key) and (b) En-Seung provides an improved and more efficient mechanism to allow the users to view / replay the digital content at their convenience wherein the terminal unit (or the replay device) is capable to directly descrambled the protected digital content by using an decryption key (i.e. temporary validation key), which is encrypted by a user key (or *corresponding to TECM key in Tsuria*), without the need to transfer the received / encrypted digital content back to the first device for decrypting and replaying the recorded digital content (En-Seung: Abstract / Line 10 – 16 and Column 16 Line 42 – 51 & Figure 23B)).

(d) obtaining in said second device said descrambling key from said rebundled descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23 – 29 & comment on (c)); and

(e) descrambling, in said second device, said scrambled data component using said descrambling key (En-Seung : Abstract / Line 10 – 14 and Column 8 Line 23 – 29 & Figure 23B / Element S570).

As per claim 2, Tsuria teaches (a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and (b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key (Tsuria: Column 10 Line 36 – 40).

As per claim 3, Tsuria teaches said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device (Tsuria: Column 3 Line 1 – 8, Column 8 Line 53 – 55 and Column 7 Line 5: See commonly assigned <both are from the same assignee NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the U.S. Patent 5,481,609, to Cohen et al., Column 1 Line 62 – 67).

As per claim 4, Tsuria teaches the step of rebundling is performed within a first smart card coupled to said first device (Tsuria: Column 7 Line 1 – 9 and Column 6 Line 66 – Column 7 Line 1) and the steps of obtaining and descrambling are performed within a second smart card coupled to said second device (Tsuria: Column 7 Line 5: See commonly assigned <both are from the same assignee NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the U.S. Patent 5,481,609, to Cohen et al., Figure 3 Element 30 / 32 and Column 178 Line 21 – 23).

As per claim 5, Tsuria teaches initializing said first device within said network (Tsuria: Column 8 Line 29 – 43 & Figure 1: the first device is IRD (Integrated Recording Decoder) which directly interfaces with the SDDS broadcasting system to discourage unauthorized duplication and subsequent play-back / recording).

As per claim 7, Tsuria as modified teaches a re-encryption key is pre-stored in a smart card coupled to said first device or in said first device (Tsuria: Column 8 Line 30 – 31). Tsuria further teaches a re-encryption key is a public key (Tsuria: Column 3 Line 1 – 8, Column 8 Line 53 – 55 and Column 7 Line 5: See commonly assigned < both are from the same assignee NDS Ltd. Inc.> and fully incorporated into Tsuria by reference the U.S. Patent 5,481,609, to Cohen et al., Column 1 Line 62 – 67). Accordingly, Tsuria as modified teaches: a public key is pre-stored in a smart card coupled to said first device or in said first device.

As per claim 8, Tsuria teaches said descrambling key is one of encrypted using a private means if said scrambled program is received from prerecorded media or protected by a private means if said scrambled program is received from a service provider (Tsuria: Column 7 Line 50 – 57).

As per claim 14, Tsuria as modified further teaches the first device is an access device and wherein the second device is a presentation device (Tsuria: Figure 1, Column 3 Line 1 – 8 and En-Seung: Column 3 Line 9 – 13, Column 6 Line 37 – 40 and Abstract / Line 10 – 18).

As per claim 17, the claim limitation(s) encompasses the same scope as described in claim 1 and claim 3 (Examiner notes the access device is considered as the first device and the

presentation device is considered as the second device). See same rationale addressed above in rejecting claim 1 and claim 3.

As per claim 20, Tsuria as modified teaches the signal output transmits identification data associated with the access device and copy control information along with the re-encrypted descrambling key (Tsuria: Column 1 Line 60 – 67 and Column 2 Line 63 – Column 3 Line 5).

As per claim 22, Tsuria as modified teaches the key information corresponding to entitlement control messages, and further comprises the key information corresponds to entitlement control messages, and further comprising the step of obtaining a descrambling key from the entitlement control messages, and the descrambling step comprises descrambling the program signal using the descrambling key (Tsuria: Column 7 Line 48 – 57).

As per claim 23, the claim limitations are met as the same reasons as that set forth above in rejecting claim 3 – Examiner notes, first of all, the public / private key pair should be used as a pair between the first device and the second device; as far as which device (the 1st device or the 2nd device) uses the private key is merely a obvious design choice – for example, claim 3 and claim 23 recites using the public key and the private key at the first device (i.e. access device) respectively (or interchangeably) and therefore Examiner notes this claim feature holds no significance of the patentable feature).

As per claim 24, the claim limitations are met as the same reasons as that set forth above in rejecting claim 19.

2. Claims 6 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (U.S. Patent 6,178,242), in view of En-Seung et al. (U.S. Patent 6,892,306), and in view of Wasilewski et al. (U.S. Patent 5,870,474).

As per claim 6, Tsuria as modified does not disclose expressly initializing comprises the step of receiving a public key from a conditional access provider.

Wasilewski teaches initializing comprises the step of receiving a public key from a conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line 38 – 43).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewski within the system of Tsuria as modified because (a) Tsuria teaches protection mechanisms for producing, recording and replaying scrambled digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) Wasilewski teaches a control system for providing secure transmission of recording digital data stream (such as "movie on demand") between a service provider and a customer's set top box over a digital network (Wasilewski: Column 1 Line 15 – 25).

Accordingly, Tsuria as modified teaches:

the step of initializing comprises the step of receiving said public key from a conditional access provider (Wasilewski: Column 3 Line 53 – 67 and Column 7 Line 38 – 43), said step of receiving comprising authentication of said conditional access provider (Wasilewski: Column 11 Line 4 – 5; Tsuria: Column 8 Line 30 – 31).

As per claim 18, Tsuria as modified does not teach the public key is periodically received from a conditional access provider.

Wasilewski teaches the public key is periodically received from a conditional access provider (Wasilewski: Column 7 Line 38 – 40 and Column 10 Line 4 – 12). See same rationale of combination applied herein as above in rejecting the claim 6.

3. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (U.S. Patent 6,178,242), in view of En-Seung et al. (U.S. Patent 6,892,306), and in view of Smyers et al. (U.S. Patent 5,948,136).

As per claim 19, Tsuria as modified does not teach the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device.

Smyers the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device (Smyers: Column 4 Line 38 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Smyers within the system of Tsuria as modified because (a) Tsuria teaches protection mechanisms for producing, recording and replaying scrambled digital data stream (Tsuria: Column 1 Line 60 – 63) and (b) Smyers teaches providing hardware authentication mechanism to enhance communication securities between two devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

=====

/Longbit Chai/

Longbit Chai E.E. Ph.D
Primary Examiner, Art Unit 2431
1/12/2011

=====